# Telephone Banking

Consider the following procedures at each examination. Examiners are encouraged to exclude items deemed unnecessary. This procedural analysis does not represent every possible action to be taken during an examination. The references are not intended to be all-inclusive and additional guidance may exist. Many of these procedures will address more than one of the Standards and Associated Risks. For the examination process to be successful, examiners must maintain open communication with bank management and discuss relevant concerns as they arise.

**IMPORTANT**
**The following telephone banking procedures should be considered at each examination where telephone banking activity is encountered. The procedures should be used in conjunction with the Telephone Banking section in the Electronic Banking supplement to the DOS Examination Manual. Examiners are encouraged to streamline the procedures when possible. For example, procedures may be omitted when a service bureau maintains all equipment and performs the majority of activities for a serviced institution. Items relevant only to in-house systems are identified by [I], while those that pertain only to a serviced environment are identified with [S]. Items that do not apply should be answered N/A. Examiners are encouraged to contact information systems specialists or subject matter experts if additional guidance is necessary.**

## PRELIMINARY REVIEW

1 Request a detailed system description (i.e., topology) and user's manual.

2 Identify activities that can be performed over the touch-tone telephone.

3 Request printouts of the system's configuration screens.

4 Review the servicer's most recent regulatory examination or third-party review for telephone banking deficiencies.

5 Determine if nondeposit, trust, and credit card information/transactions are available over the phone. If so, ascertain if these are separate, distinct systems.

## MANAGEMENT

6 Determine whether management adequately tested the system prior to deployment or any significant modifications. Determine if management periodically reviews call volume to monitor system capacity and usage.

7 Determine if management has obtained adequate insurance coverage of telephone banking activities, including vendor activities.

8 Determine if management entered into formal contracts with vendors and data servicers which provide telephone banking products and services. Evaluate the comprehensiveness of the contracts. [S]

## AUDIT

9 Determine if the bank's internal or external auditor reviews the telephone banking system.

## PASSWORD ADMINISTRATION

10 Verify that management has established adequate controls over PIN administration. Identify who has the ability to reset customer PINs.

11 Determine which bank employees have the ability to access and/or view customer PIN information.

## ACCOUNT AND SYSTEM ADMINISTRATION

12 Prior to enabling telephone access, determine if written authorization is required from each customer and that customer information is verified.

13 Determine how customer accounts are linked together to allow transfers between accounts. Describe how joint accounts are maintained on the system.

14 Determine if unique login IDs restrict which functions a user can perform. Verify that the system administrator login ID and password have been changed from the default vendor setting.

15 Identify the system administrator and describe the administrator's responsibilities. If system administration can be performed remotely through the VRU, verify that adequate controls exist to restrict remote access.

16 Determine the frequency that the following activity and exception reports are produced and reviewed by an independent party.

16A PIN changes.

16B Changes to narrative product/service information.

16C New, deleted, or changed account profiles.

16D Failed access attempts.

16E Incomplete transactions and unusual activity.

## COMPUTER OPERATIONS

17 Determine if adequate safeguards exist to ensure only authorized personnel have access to the VRU and the PC which maintains the telephone banking program. Verify if supervisor access or a special password is required to access or change the VRU voice scripts.

18 Determine if the VRU or server is directly connected to the bank's mainframe computer. If so, describe the security features which prevent the mainframe from unauthorized access.

19 Assess the adequacy of back-up procedures.

20 Determine how management monitors programming changes. [I]

## TELECOMMUNICATIONS

21 Determine if the system is batch processed or on-line, real-time.

22 If batch processed, determine how frequently the database is refreshed with new data. Describe controls in place to verify the integrity and accuracy of the information uploaded and downloaded to/from the master file.

23 Determine if leased or dedicated lines are used for better security when transmitting data to/from the data servicer. If dial-up lines are used, determine the identification method to authorize the connection. [S]

24 Assess how vendor updates are performed to the system. Determine if adequate controls exist over remote vendor access and that all changes are reviewed the next day.

25 Determine if the bank established a maximum connection time per call before the system disconnects the caller.

26 Determine if the bank limits the number of unsuccessful attempts to access the system before the caller is disconnected.

## FUNDS TRANSFER / BILL PAYMENT

27 Determine if account activity conducted over the telephone is reflected on other platforms/systems.

28 Determine if customers can transfer funds to accounts at other financial institutions. If so, describe controls over authorization.

29 For both the bill pay and funds transfer programs, describe how payees are added, changed, or deleted from a customer's profile. Determine if signed authorizations are required for each payee and how the bank verifies the legitimacy of each payee. Determine if customers can set up transfers or establish new bill pay merchants over the telephone and immediately transfer money from their account(s).

30 For merchant payments made on behalf of multiple customers, determine the method used to provide merchants with relevant customer information (e.g., account name, number, and amount of payment).

31 If the bank uses third-party bill payment vendors, determine that management has entered into a formal contract. Verify that the contract governs the following, at a minimum.

31A Confidentiality.

31B Back up arrangements.

31C Fees and service charges.

31D Liability.

31E Insurance coverage.

31F Ownership of funds.

32 Determine procedures to withdraw bill payment funds from customer accounts. If a suspense account is used to hold funds before transferring payment to merchants, verify that the account is regularly reconciled.

33 If customers can request bank checks (e.g., treasurer's checks, cashier's checks) via the telephone, determine if adequate controls are in place covering the storage, printing, and distribution of checks.

## FAXBACK REQUESTS

34 If the bank offers faxback services, assess the procedures addressing customer requests for faxes via the touch-tone telephone.

35 Determine if management has restricted the number of pages that can be faxed per request.

## LOAN APPLICATIONS

36 Assess the procedures for validating automated loan applications and authenticating both bank and non-bank customers.

## SERVICE BUREAUS

*(Completed only at IS examinations of data centers.)*

37 Determine how the service bureau protects each bank's data from unauthorized access, especially if shared VRUs are used for routing customer requests among multiple banks.